8

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/007,019	10/19/2001	Ralph A. Gilman	A6425/T45100	7918

32588 7590 06/28/2005

APPLIED MATERIALS, INC.
2881 SCOTT BLVD. M/S 2061
SANTA CLARA, CA 95050

EXAMINER	
COLIN, CARL G	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 06/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/007,019	**Applicant(s)** GILMAN ET AL.	
	Examiner Carl Colin	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 October 2001* .

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10/19/2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)	4) □ Interview Summary (PTO-413) Paper No(s). _____ .
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) □ Notice of Informal Patent Application (PTO-152)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *see att* .	6) □ Other:

DETAILED ACTION

1. Pursuant to USC 131, claims 1-23 are presented for examination.

Specification

2. The specification is also objected to because of the following informalities: there is lack of consistency between the reference numbers and the description. For instance, reference number 165 on page 18, line 2 is referred to as a portable computing device whereas page 18, line 4 refers to it as a workstation. Applicant's cooperation is requested in correcting any similar errors of which applicant may become aware in the specification.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claim 5 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3.1 Claim 5 recites "the method of claim 5..." There is insufficient antecedent basis for the limitation in the claim since claim 5 is dependent on itself.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.1 **Claims 8-9, 13, 15,** and **20-23** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,519,568 to **Harvey et al** in view of US Patent Publication 2002/0090089 to **Branigan et al**.

4.2 **As per claims 20-21, Harvey et al** discloses a networked system comprising: a private communication network, a virtual private network (VPN) node coupled to said private network (column 17, lines 22-39); a supplier client system coupled to the private network through said VPN node (column 17, lines 22-39); and discloses a VPN hub 78 connected to a node 76 to create a secure enclave within the intranet that meets the recitation of a VPN hub coupled to said private network, wherein said VPN node and VPN hub are configured to create an isolation pipe therebetween within said private network (column 17, lines 22-39); **Harvey et al** discloses a firewall coupled to the private network, to said VPN hub and to a public network, said firewall providing security features that enable said private network to connect to the public network (column 23, lines 35-60). **Harvey et al** substantially discloses said VPN node is configured to receive a request from said supplier client system for viewing a desired Web page sent over the public network and pass said request on to said VPN hub (column 23, lines 35-67; column 24, lines 18 through column 25, line 6) and discloses said VPN hub is configured to pass said request from said VPN node to said firewall; and said firewall is configured to transmit said request over said public network (column 23, lines 35-67). The difference with the claimed limitation is that **Harvey et al** discloses a central hub or e-hub on the other side of the operator's Intranet in the exemplary embodiment, but suggests that a central hub could be located within a secure Intranet or within an associated secure enclave and also suggests using point to point protocol (column 8, lines 31-46). It is apparent to one skilled in the art that using a e-hub in the operator private network to secure communications going through the Internet would have been an obvious modification. **Branigan et al** in an analogous art discloses an improved network security of a wireless network connected to a wired network, the wireless network is connected to a VPN hub and the network protocol used is point to point tunneling protocol in order to protect the information traveling over the private network (page 3, paragraph 18). **Branigan et al** discloses the claimed limitation of claim 21 (pages 2-3, paragraphs 9-18) but does not explicitly disclose using a firewall and is silent about the detail of the resource network. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the operator's private network in **Harvey et al** to implement a VPN hub and point to point tunneling protocol in the operator's private network in order to protect the information traveling over the private network as taught by **Branigan et al**. One skilled in the art would have been motivated to make such a modification because the point to point tunneling protocol permits all traffic to travel between the two points in an encryption format as known in the art and therefore protect the information traveling over the private network between the user and the hub using tunneling protocol as suggested by **Branigan et al** (pages 2-3, paragraphs 9-18).

As per claims 8-9, Harvey et al substantially discloses in a customer network comprising a plurality of customer client systems, at least one customer server system and a customer firewall where said plurality of customer client systems are communicatively coupled to said server system using a first physical connection type, said server system is communicatively coupled to said firewall and said customer firewall is communicatively coupled to a public network, a method of allowing end-to-end secure communication from a supplier client system located behind said firewall to a supplier server system accessible over said public network (column 17, line 55 through column 18, line 10), said method comprising: **Harvey et al** discloses using different connection types because the secure enclave and a central hub could be integrated on any Intranet depending on design choice as suggested in (column 8, lines 31-46) that meets the recitation of connecting said supplier client system to said customer network using a second physical connection type that is different from said first physical connection type; transmitting said data from said customer firewall to said public network; and receiving said data at said supplier server system (column 17, line 55 through column 18, line 10). **Harvey et al** discloses a hub can be located within the operator's intranet using point to point communication (column 8, lines 31-46) and preferably through firewall (column 23, line 35 through column 24, line 5) but does not explicitly disclose using a tunneling protocol for establishing an isolation pipe between said supplier client system and a server system of said customer network. The use of tunneling protocol is discussed above in claims 20-21. Therefore, claims 8-9 are rejected on the same rationale as the rejection of claims 20-21.

Claim 13 recites similar limitation to the rejected claim 21 except for stating authenticating communication between said client system and a wireless access point of said first private network (see **Branigan et al**, page 2, paragraphs 14-15). Claim 13 further recites that the client system request is routed through said first private network, in order, from said client system, to said wireless access point, to a virtual private network node, to a virtual private network hub, and through said firewall and wherein said request is routed from said virtual private network node to said virtual private network hub using a tunneling protocol. **Harvey et al** discloses communication from client to a node to a VPN hub (see fig. 4-6) and (column 8, lines 31-46) and through firewall (column 23, lines 35-60). **Harvey et al** further discloses the client system can be a wireless network. Therefore, the access point is inherent in the wireless protocol. **Branigan et al** also discloses a request from the client in the order as recited in claim 1 using a tunneling protocol (see **Branigan et al**, figures 1-2 with detailed description) except for being silent about firewall, which is well known in the art for controlling data entering and leaving a network, the use of firewall would have also been an obvious modification to one skilled in the art for controlling traffic entering and leaving the intranet as well known art and as suggested by **Harvey et al**. The combination of **Harvey et al** and **Branigan et al** disclose the claimed method of claim 13 and therefore is rejected on the same rationale as the rejection of claim 21.

Claim 15 recites similar limitation to the rejected claims 20 and 21. **Harvey et al** discloses creating secure point to point protocol using VPN and transmitting request from said supplier client system to said firewall and transmit said desired Web page from said Internet through said firewall to said supplier client system create a secure pipeline within said private communication network tunnel to transmit said request from said supplier client system to said firewall and transmit said desired Web page from said Internet through said firewall to said supplier client system (column 23, lines 35-67; column 24, lines 18 through column 25, line 6) and access from and to company intranets are protected by firewall (column 23, lines 35-60). Therefore, claim 15 is rejected on the same rationale as the rejection of claims 20-21.

As per claim 22, Harvey et al discloses the limitation of wherein said VPN node is configured to transmit only requests generated in said secure Internet protocol to said VPN hub (column 23, lines 56-60).

As per claim 23, Harvey et al discloses using secure Internet protocols such as HTTPS that meets the recitation of wherein said secure Internet protocol is the Secure Sockets Layer (SSL) protocol (column 15, lines 45-51).

5. **Claim 14** is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,519,568 to **Harvey et al** in view of US Patent Publication 2002/0090089 to **Branigan et al** as applied to claims 1, 8, 13, 20-21 above and further in view of Non-Patent Literature *(Applicant's*

Disclosure): BLOSS et al, "E-Manufacturing Opportunities in Semiconductor Proceessing" Semiconductor International, pp. 88-96 (July 2001).

5.1 **As per claim 14,** both references substantially disclose the claimed method of claim 13. None of the references explicitly disclose that the client system is located in a cleanroom of a semiconductor fabrication facility and said wireless access point is located outside said cleanroom. **Bloss et al** in an analogous art discloses the importance of maintaining security in a semiconductor facility and further discloses an architecture that shows a supplier separate from the access point for access control and security measure (see figures 2-3). It is well known in the art that when security of a company industry or enterprise is a major concern that the access points are in a secure maintenance room, which makes it an easier access for maintaining and repairing and in addition provides security towards the equipment. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the method as combined above to a semiconductor fabrication facility and said wireless access point is located outside the cleanroom in order to protect physical access to the equipment by unauthorized users as suggested by **Bloss et al**. One skilled in the art would have been motivated to make such a modification to control access to the equipment for maintaining and repairing and in addition to provide security towards the equipment so that unauthorized users don't have access to tamper with the equipment.

6. **Claims 10-12 and 16-19** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,519,568 to **Harvey et al** in view of US Patent Publication 2002/0090089 to

Branigan et al as applied to claims 8-9 above and further in view of Non-Patent Literature Richard E. **Smith**, "Internet Cryptography", January 2000, Addison Wesley Longman Inc., 4th printing, pages 145-147.

As per claims 10 and 16, both references substantially disclose the claimed method of claims 8-9. **Branigan et al** discloses a tunnel mode that supports encryption. Layer 2 and layer-3 tunneling protocol are well known in the art in Ipsec protocol, therefore **Branigan et al** did not provide details about how to encrypt the header and the body of the packet. As known in the art, in tunnel mode the entire IP packet is encrypted and embedded in another IP packet and as the packet arrives at the end of the tunnel the header is unencrypted so that the packet can be routed to its destination while the IP packet remains encrypted to maintain the security of the transmission of the packet over the public network (See **Smith**, pages 145-147). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the encrypted point to point tunnel between the client and the server as combined above to establish an encrypted tunnel between the client and the server as well known in the art wherein both the network transmission header and already encrypted data portions of each packet associated with said formatted request is encrypted at said node using a VPN-level encryption protocol prior to being transmitted through said isolation pipe and then decrypted at said hub/firewall such that the header is unencrypted and the data portion is encrypted using only the SSL protocol prior to being transmitted over the public Internet. One skilled in the art would have been motivated to make such a modification to establish an encrypted tunnel as suggested in **Smith** and maintaining security of the transmission of the packet over the public network to reduce the ability of unauthorized third parties to tamper,. listen or interfere with the packet.

As per claims 11 and **19, Harvey et al** discloses using secure Internet protocols such as HTTPS that meets the recitation of wherein said secure Internet protocol is the Secure Sockets Layer (SSL) protocol (column 15, lines 45-51).

Claims 12 and **17** recite some of the limitations found in the rejected claim 13 and they are rejected on the same rationale as the rejection of claim 13.

As per claim 18, Harvey et al discloses the limitation of wherein said VPN node is configured to transmit only requests generated in said secure Internet protocol to said VPN hub (column 23, lines 56-60).

7. **Claims 1-7,** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,519,568 to **Harvey et al** in view of US Patent Publication 2002/0090089 to **Branigan et al,** in view of Non-Patent Literature *(Applicant's Disclosure)*: BLOSS et al, "E-Manufacturing Opportunities in Semiconductor Proceessing" Semiconductor International, pp. 88-96 (July 2001), and in view of Non-Patent Literature Richard E. **Smith**, "Internet Cryptography", January 2000, Addison Wesley Longman Inc., 4th printing, pages 145-147.

Claim 1-7 recite similar limitations as found in the rejected claims 8-11 and 14. Therefore, claims 1-7 are rejected on the same rationale as the rejection of claims 8-11 and 14.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses use of tunneling protocol, Ipsec encapsulation, VPN, etc..

US Patents: 6,104,716 Crichton et al; 6,507,908 Caronni ; 6,760,330 Tahan.

US Patent Publications: US 2003/0031320 to Fan et al; US 2002/0010866 Mc Cullough et al; US 2002/00783870 Tahan; US 2002/0091801 Lewin et al.

8.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin
Patent Examiner
June 20, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100